Georgia Technology Authority

Password Management Systems

POLICY NUMBER: 9.7.3	EFFECTIVE DATE: 11/01/06

PURPOSE

To describe the capabilities for password management to provide sufficient password security for computing resources in the State of Georgia.

SCOPE

Any computing and networking resources within the mandate of the Georgia Technology Authority (GTA). This policy covers the method of ensuring that passwords are of a sufficient quality to be considered safe to use.

POLICY

Password management systems should be deployed where feasible to provide a reliable, effective method of ensuring the use of high quality passwords.

STANDARD

Each Agency is responsible for the strength of the passwords used to authenticate its users. Where possible, Agencies should deploy automated password checking systems to ensure all passwords meet the applicable standards. Where this is not possible, the Agency is responsible for periodic password strength assessments using password cracking tools on the password stores. These assessments must be conducted at least monthly.

GUIDELINES

Physical Password Security

Within any specific computing environment the ability of general users to access the files containing passwords should be limited. Access of password files by users should be monitored for unauthorized activity where possible.

Best Practice Features of Password Management

- Individual passwords should be unique per user and be accessible for accountability.
- Provide for creating high quality passwords
- Allow users to create their own passwords and include a confirmation method for possible input errors.
- Where users maintain their own password, enforce password change schedules and password policies based on section 9.3.1.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

In the case of an information system managed by a third party, the Agency CIO can, in concurrence with the information owner, make a determination that the third party's security controls meet or exceed this standard. This exception must be based on an assessment of the third party's controls and documented in writing. Please see policies 4.2.2, 4.3.1, and 8.1.5 for further information.

TERMS AND DEFINITIONS (see Section 2)